# FortiClient EMS for Chromebooks - Admin Guide

Version 1.2.4

**FORTINET DOCUMENT LIBRARY**
http://docs.fortinet.com

**FORTINET VIDEO GUIDE**
http://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTIGATE COOKBOOK**
http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**
http://www.fortinet.com/training

**FORTIGUARD CENTER**
http://www.fortiguard.com

**END USER LICENSE AGREEMENT**
http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdocs@fortinet.com

January 29, 2018
FortiClient EMS for Chromebooks 1.2.4 Admin Guide
04-124-436863-20180129

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2018-01-29 | Initial release. |
| | |
| | |

# Introduction

FortiClient Enterprise Management Server for Chromebooks (FortiClient EMS for Chromebooks) is a security management solution that works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

FortiClient EMS for Chromebooks is designed to meet the needs of small to large enterprises that provide web filtering for Google Chromebook users. Benefits of deploying FortiClient EMS for Chromebooks include:

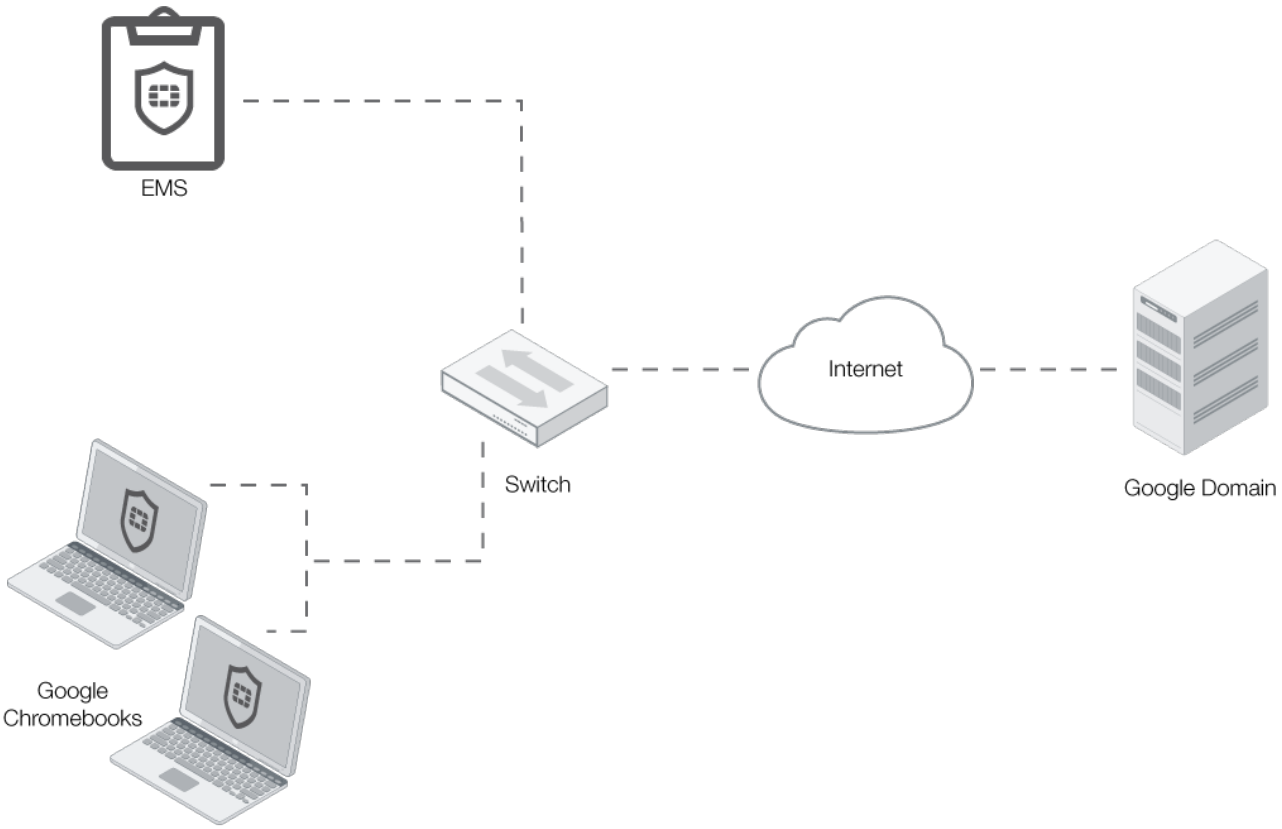
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints
- Updating profiles for Google Chromebook users regardless of access location
- Monitoring Google Chromebook endpoints

## FortiClient EMS for Chromebooks components

FortiClient EMS for Chromebooks provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS for Chromebooks to filter web content endpoint users view on Google Chromebooks.

The following table lists the FortiClient EMS for Chromebooks components.

| Component | Description |
|---|---|
| **FortiClient EMS for Chromebooks** | Manages web filtering on Google Chromebook endpoints with the FortiClient Web Filter extension installed that connect to your Google domain. It includes the following software:<br>• Console software that manages security profiles and Chromebook endpoints.<br>• Server software that provides secure communication to and from Chromebook endpoints and the Google Admin console. |
| **Database** | Stores security profiles, events, and user information retrieved from the Google Admin console. The SQL database is installed as part of the FortiClient EMS for Chromebooks installation. |
| **FortiClient Web Filter extension** | Communicates with FortiClient EMS for Chromebooks and enforces web filtering on Google Chromebook endpoints. |




FortiClient EMS for Chromebooks allows you to:

- Establish and enforce security profiles
- Manage security profiles from an integrated management console
- Obtain a consolidated view of multiple security profiles across all endpoints in your Google domain
- Monitor endpoints' web browsing activity

## FortiClient EMS for Chromebooks and Fortinet Endpoint Security Management

FortiClient EMS for Chromebooks is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

## Documentation

You can access FortiClient EMS for Chromebooks documentation from the following link: docs.fortinet.com/ems/admin-guides

The FortiClient EMS for Chromebooks documentation set includes the following:

- *FortiClient EMS for Chromebooks 1.2.4 Release Notes*

  This document describes new features and enhancements in FortiClient EMS for Chromebooks for the release and lists any known issues and limitations. This document also defines supported platforms and minimum system requirements.
- *FortiClient EMS for Chromebooks 1.2.4 QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS for Chromebooks system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS for Chromebooks system.
- *FortiClient EMS for Chromebooks 1.2.4 Administration Guide*

  This document describes how to set up FortiClient EMS for Chromebooks and use it to manage Chromebook endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor Chromebook endpoints.
- *FortiClient EMS for Chromebooks Upgrade Paths*

  This document provides upgrade path information for different versions of FortiClient EMS for Chromebooks.

# What's New

The following is a list of new features and enhancements in FortiClient EMS for Chromebooks 1.2.

## FortiClient EMS for Chromebooks 1.2.4

FortiClient EMS for Chromebooks 1.2.4 does not contain new features or enhancements.

## FortiClient EMS for Chromebooks 1.2.3

FortiClient EMS for Chromebooks 1.2.3 does not contain new features or enhancements.

## FortiClient EMS for Chromebooks 1.2.2

### Redesigned navigation menu

The left navigation menu has been redesigned to provide easier access to the content pane on the right. The top menu has also been merged into the left navigation menu.

### New Dashboard

The new Dashboard includes new chart designs and easier access to information and alerts. Administrators can customize the dashboard by moving widgets around. See Dashboard on page 48.

## FortiClient EMS for Chromebooks 1.2.1

FortiClient EMS for Chromebooks 1.2.1 does not contain new features or enhancements.

# FortiClient EMS for Chromebooks 1.2.0

## Pre-login banner

The pre-login banner can be used to display a message on the login page for FortiClient EMS for Chromebooks before the user logs in. Users must accept the banner message before they can log in. See Configuring the login banner on page 67.

## Separate license for EMS Chromebook support

Users can purchase a license applicable for FortiClient EMS and FortiClient EMS for Chromebooks. Alternatively, they can purchase licenses only applicable for FortiClient EMS for Chromebooks for a lower price.

# Get Started

This section provides an overview of how to perform the following tasks after you install and license FortiClient EMS for Chromebooks.



This section also includes a description of how FortiClient EMS for Chromebooks and FortiClient work with Google Chromebooks after setup is complete.

## Configuring FortiClient EMS for Chromebooks

**To configure FortiClient EMS for Chromebooks:**

1. Start and log into FortiClient EMS for Chromebooks. See Starting FortiClient EMS for Chromebooks and logging in on page 21.
2. Add SSL certificates. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 68.
3. Configure FortiClient EMS for Chromebooks settings. See System Settings on page 66.
4. Configure user accounts and permissions. See Administrators on page 61.

## Configuring the Google Admin console

Following is an overview of how to configure the Google Admin console to prepare for adding the Google domain to FortiClient EMS for Chromebooks. The document assumes you have created the Google domain.

**To configure the Google Admin console:**

1. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 29.
2. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 30.
3. Add root certificates. See Adding root certificates on page 31.
4. Configure unique service account credentials. See Configuring unique service account credentials on page 40.
5. Disallow incognito mode. See Disallowing incognito mode on page 34.

# Deploying profiles to Chromebooks

Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks. After you add the extension in the Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs into the Chromebook.

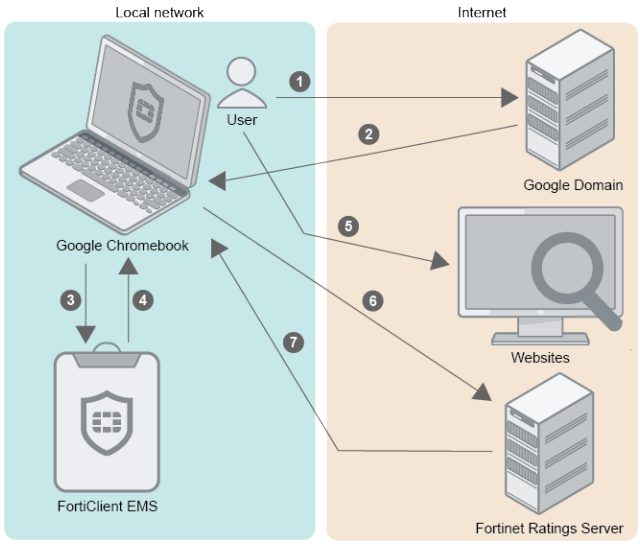
**To deploy profiles to Chromebooks:**

1. Add the Google domain. See Adding Google domains on page 50.
2. Define web filtering options in one or more profiles. See Configuring profiles on page 54.
   You can enable Safe Search in profiles.
3. Assign profiles to domains to deploy profiles to the FortiClient Web Filter extension on Chromebook endpoints. See Assigning profiles to Google Chromebooks on page 56.
4. Verify the FortiClient Web Filter extension. See Verifying the FortiClient Web Filter extension on page 37.
5. View Google domains and Google users. See Viewing domains on page 50.

# How FortiClient EMS for Chromebooks and FortiClient work with Chromebooks

After you install and configure FortiClient EMS for Chromebooks, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS for Chromebooks.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS for Chromebooks.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.
7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category result with the profile to determine whether to allow the Google Chromebook user to access the URL.


Local network
Internet
User
Google Chromebook
Google Domain
Websites
FortiClient EMS
Fortinet Ratings Server
1
2
3
4
5
6
7

# Installation Preparation

This section helps you prepare to install FortiClient EMS for Chromebooks. Before installing FortiClient EMS for Chromebooks, be aware of the following information.



Before installing FortiClient EMS for Chromebooks, it is recommended you read the *FortiClient EMS for Chromebooks Release Notes* available on http://docs.fortinet.com/ems/release-information to become familiar with relevant software components and other important information about the product.

## Licenses

This section describes licensing options available for FortiClient EMS for Chromebooks. It provides information about the number of supported Google Chromebooks for each type of license to help determine which license best suits your needs.

### FortiClient EMS for Chromebooks

FortiClient EMS for Chromebooks supports the following types of licenses:

- Free trial license
- Purchased license

#### Free trial license

When you install FortiClient EMS for Chromebooks, the free trial license is enabled by default. The free trial license supports ten Google Chromebook users. FortiClient EMS for Chromebooks consumes one license count for each logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

### Purchased license

Each purchased license allows management of one Google Chromebook user. You must purchase a minimum of 100 Google Chromebook user licenses and can have these EMS licenses for a maximum three year term. You can specify the number of Google Chromebook users and the term duration at time of purchase. FortiClient EMS for Chromebooks uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

An email is sent when you are running out of licenses. Additionally, a log entry is entered when a client is refused connection due to unavailable licenses.

## Component applications

Common services or applications do not require a license.

During the installation of common services required for FortiClient EMS for Chromebooks, you are not asked for license information.

# Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS for Chromebooks and its associated applications on your server. The required ports and services enable FortiClient EMS for Chromebooks to communicate with endpoints and servers running associated applications.

| Communication | Service | Protocol | Port |
|---|---|---|---|
| **Apache** | HTTPS | TCP | 443 |
| **SQL server** | | | |
| **FortiClient on Chrome OS**<br>• Connection to Profile Server. | | | 8443 (default)<br>You can customize this port. |

# Management capacity

FortiClient EMS for Chromebooks is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested host system hardware configurations for FortiClient EMS for Chromebooks. The suggested configurations depend on the number of endpoints FortiClient EMS for Chromebooks is managing.

You need at least 200 GB of disk space available.

| Maximum number of managed endpoints | Number of virtual CPUs | Memory (RAM) (in GB) | Suggested keep alive interval |
|---|---|---|---|
| 10000 | 2 | 8 | Default |
| 20000 | 4 | 8 | Default |
| 30000 | 4 | 8 | 120 seconds |
| 40000 | 4 | 8 | 120 seconds |
| 50000 | 4 | 8 | 120 seconds |
| **Suggested minimum system hardware for FortiClient EMS for Chromebooks:** | | | |
| 75000 | 8 | 16 | 120 seconds |

For the purpose of this table, an Intel i5 processor with two cores and two threads per core is considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

# Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

| Checklist | Readiness factor |
|---|---|
| | Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS for Chromebooks. Installation may be slow or disrupted while these programs are active. Note a server may be vulnerable to attack when you uninstall or disable security applications. |
| | It is recommended to sync the time to the Google server time. |
| | Confirm required services and ports are enabled and available for use by FortiClient EMS for Chromebooks. |
| | Ensure no conflict exists with port 443 for the Apache service to function properly. |
| | Ensure no conflict exists with port 8443 for the EMS service to function properly. |

# G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

The G Suite account is different from the free consumer account. The G Suite account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a G Suite account here: https://gsuite.google.com/signup/basic/welcome#0

In the sign up process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

# SSL certificates

FortiClient EMS for Chromebooks requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where FortiClient EMS for Chromebooks is installed should have a fully qualified domain name (FQDN), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 68. You do not need to add the root certificate to the Google Admin console.

If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS for Chromebooks and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS for Chromebooks. See Adding root certificates on page 31.

# Upgrading from an earlier FortiClient EMS for Chromebooks version

FortiClient EMS for Chromebooks 1.2.4 supports upgrading from FortiClient EMS for Chromebooks 1.0.3 and later 1.0 versions. To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. Follow the procedure below.

1. (Optional) Back up the database from the EMS 1.0.x production server.
2. Install EMS 1.0.x on a staging server.
3. (Optional) Import the EMS 1.0.x database from the production server.
4. Connect FortiClient endpoints to the staging server.
5. Upgrade the staging server to EMS 1.2.4.
6. Monitor the staging server for two days.
7. Upgrade the production server to EMS 1.2.4.

# Installation and Licensing

Before you install and license FortiClient EMS for Chromebooks on a server, ensure you have:

- Reviewed Licenses on page 15
- Met the requirements listed in Required services and ports on page 16
- Completed the Server readiness checklist for installation on page 17
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS for Chromebooks, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended you install FortiClient EMS for Chromebooks on a dedicated server in a controlled environment. Installing other software applications can interfere with normal operation of FortiClient EMS for Chromebooks.

## Downloading the installation file

FortiClient EMS for Chromebooks is available for download from the following location:

Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS for Chromebooks:

`FortiClientEnterpriseManagement_Chromebook_1.2.4.<build>_x64.exe`

For information about obtaining FortiClient EMS for Chromebooks, contact your Fortinet reseller.

## Installing FortiClient EMS for Chromebooks

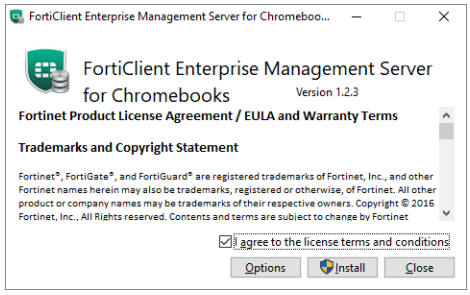
The FortiClient EMS for Chromebooks installation package includes:

- FortiClient EMS for Chromebooks
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

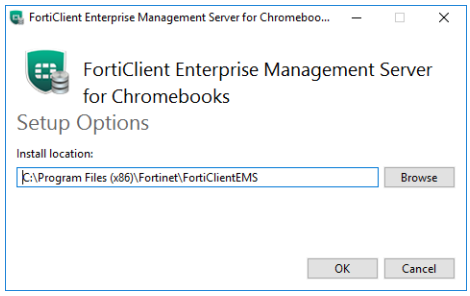
Local administrator rights and Internet access are required to install FortiClient EMS for Chromebooks.

**To install FortiClient EMS for Chromebooks:**

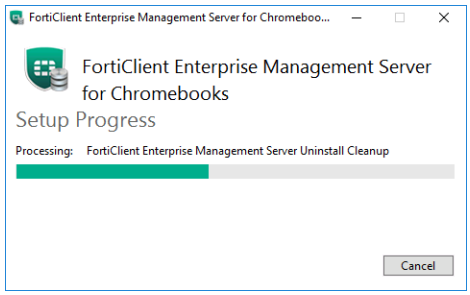
1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.



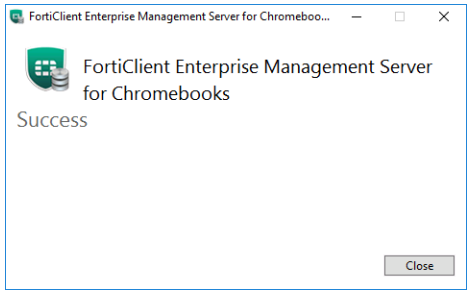

4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS for Chromebooks installation.




   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.




A *FortiClient Enterprise Management Server* icon is added to the desktop.

# Starting FortiClient EMS for Chromebooks and logging in

FortiClient EMS for Chromebooks runs as a service on Windows computers.

**To start FortiClient EMS for Chromebooks:**

1. Double-click the *FortiClient Enterprise Management Server for Chromebooks* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration* > *Administrators*.
4. Configure FortiClient EMS for Chromebooks by going to *System Settings*.

# Accessing FortiClient EMS for Chromebooks remotely

You can access FortiClient EMS for Chromebooks remotely using a web browser instead of the GUI.

**To enable remote access to FortiClient EMS for Chromebooks:**

1. Go to *System Settings* > *Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

**To remotely access FortiClient EMS for Chromebooks:**

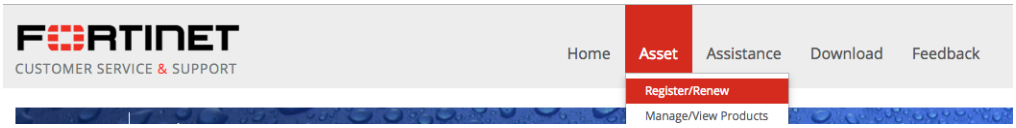
- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`

  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

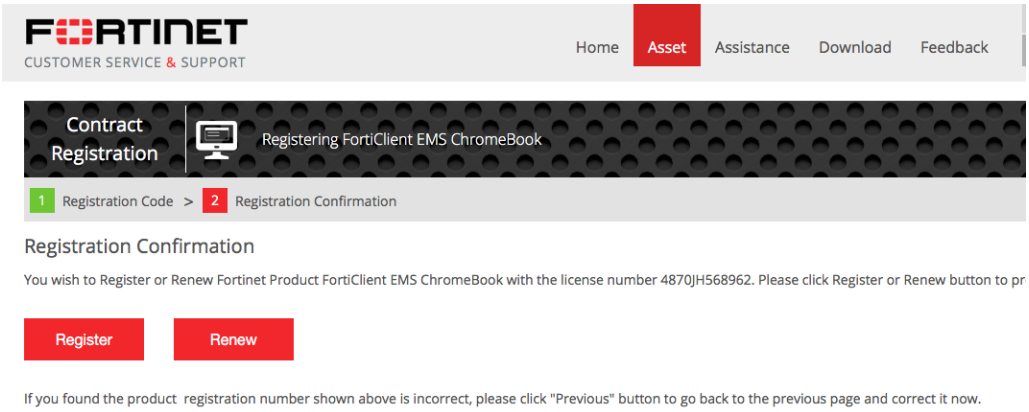
# Licensing FortiClient EMS for Chromebooks

**To license FortiClient EMS for Chromebooks:**

1. Purchase FortiClient EMS for Chromebooks from a reseller.
   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS for Chromebooks, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS for Chromebooks license.
2. Log into the Fortinet Support website.
3. Register FortiClient EMS for Chromebooks:
   a. Go to *Asset* > *Register/Renew*.

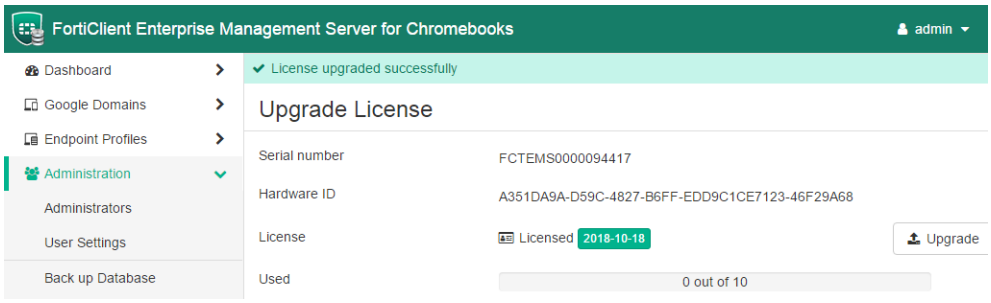



   b. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   c. Select the end user type, then click *Next*.
   d. Click *Register*.




   If you have not registered an EMS device, you are prompted to do so. This requires obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by going to *Administration* > *Upgrade License* > *Hardware ID*.
   e. In the *Product Description* field, enter a product description if desired, then enter the *Hardware ID*.
   f. Select the *Fortinet Partner* reseller, then click *Next*.
   g. Read, verify, and agree to the service's *Terms and Conditions*, then click *Next*.
   h. Verify the *Product Entitlement* list for your FortiClient EMS for Chromebooks purchase. Select the *BY ACCEPTING THESE TERMS...* checkbox, then click *Confirm*. The license file is now available to use with your FortiClient EMS for Chromebooks installation.
   i. Click *Finish*.
4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS for Chromebooks.
   b. From the left panel, select *License & Key*.
   c. From the *Available Key(s)* list, click *Get The License File* for FortiClient EMS for Chromebooks.

5. License FortiClient EMS for Chromebooks:
   a. From FortiClient EMS for Chromebooks, go to *Administration* > *Upgrade License*. Click the *Activate* button.
   b. Click the *Browse* button, select the license file, and click *Upload*. You have successfully licensed FortiClient EMS for Chromebooks.




To upgrade or renew your license, contact Fortinet Support.

## License status

The *Dashboard* > *FortiClient Status* > *System Information* widget displays your license status. Your license status can change. The options are:

| License Status | Description |
|---|---|
| Trial | If you just installed FortiClient EMS for Chromebooks, the trial license is enabled by default. You should upload the license file you purchased. |
| Non-expired license | You can upgrade the license. See License upgrades or renewals on page 64. |
| Expired license | You can renew the license. See License upgrades or renewals on page 64. |

## Extending license expiries

You can apply multiple licenses to FortiClient EMS for Chromebooks to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS for Chromebooks. After you register and apply the first license, FortiClient EMS for Chromebooks has an expiry date of September 5, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS for Chromebooks has an expiry date of September 5, 2019.

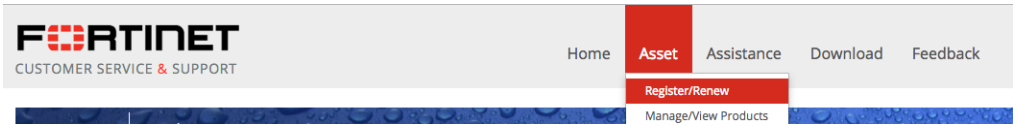
Note you must upload the second license file to FortiClient EMS for Chromebooks using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS for Chromebooks.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

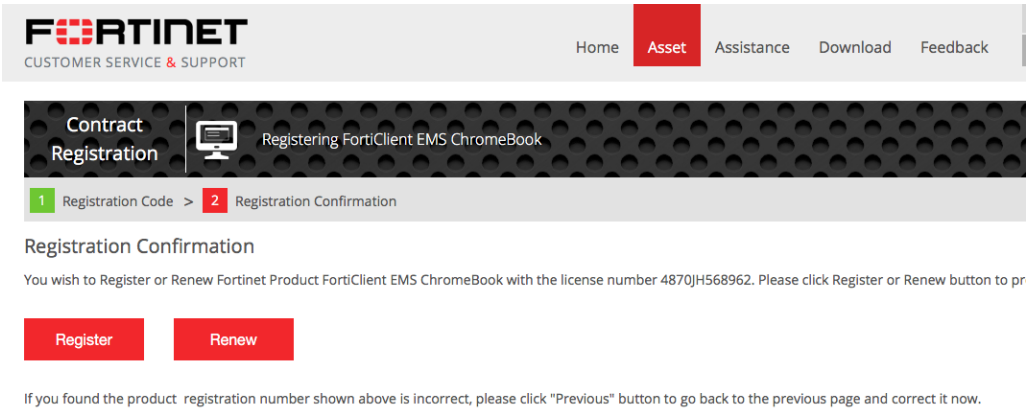
**To extend a license expiry:**

1. Purchase two FortiClient EMS for Chromebooks licenses separately from a reseller. You must purchase the licenses separately to ensure there are two registration codes. Otherwise, you cannot stack the licenses.

   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS for Chromebooks, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS for Chromebooks license.
2. Register and apply the first license to FortiClient EMS for Chromebooks as described in Licensing FortiClient EMS for Chromebooks on page 22.
3. Register the second license:
   a. Log into the Fortinet Support website.
   b. Go to *Asset* > *Register/Renew*.

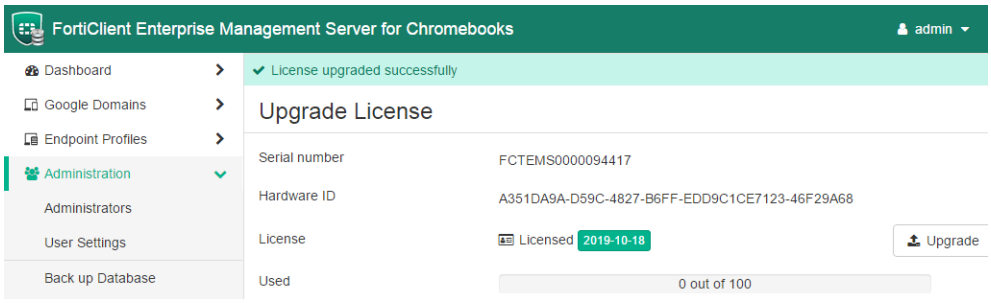



   c. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   d. Select the end user type, then click *Next*.
   e. In the *Registration Confirmation* window, click *Renew*.




   f. In the *Specify Fortinet Registration Information* window, do one of the following. You can find the serial number in the *System Information* widget in FortiClient EMS for Chromebooks.
      i. Enter the serial number in the *The Product Serial Number is* field.
      ii. Select the desired serial number in the *Product SN* list.
   g. Read, verify, and agree to the service's *Terms and Conditions*.
4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS for Chromebooks.
   b. From the left panel, select *License and Key*.
   c. From the *Available Key(s) List*, select the FortiClient EMS for Chromebooks entry. Then, click *Get The License File*.
5. License FortiClient EMS for Chromebooks:
   a. From FortiClient EMS for Chromebooks, go to *Administration* > *Upgrade License*, then click *Activate*.
   b. Click *Browse*, select the license file, and click *Upload*. You have successfully extended the license for FortiClient EMS for Chromebooks. The expiry date displayed in the *System Information* widget updates to a

year after the initial license expiry date.




## Help with licensing

For licensing issues with FortiClient EMS for Chromebooks, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

# Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS for Chromebooks ports, you can specify another port using the CLI to run the installer. You can use the following command:

| Command | Description |
|---|---|
| `RemoteManagementPort` | Port used for EMS administration. |

# Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

FortiClient EMS for Chromebooks is installed with Microsoft SQL Server Express, which has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The FortiClient EMS for Chromebooks administrator may upgrade SQL Server from Express to Standard or Enterprise edition. The database file size limit for these editions is in the PB range, which is unlimited for most practical usage.

Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

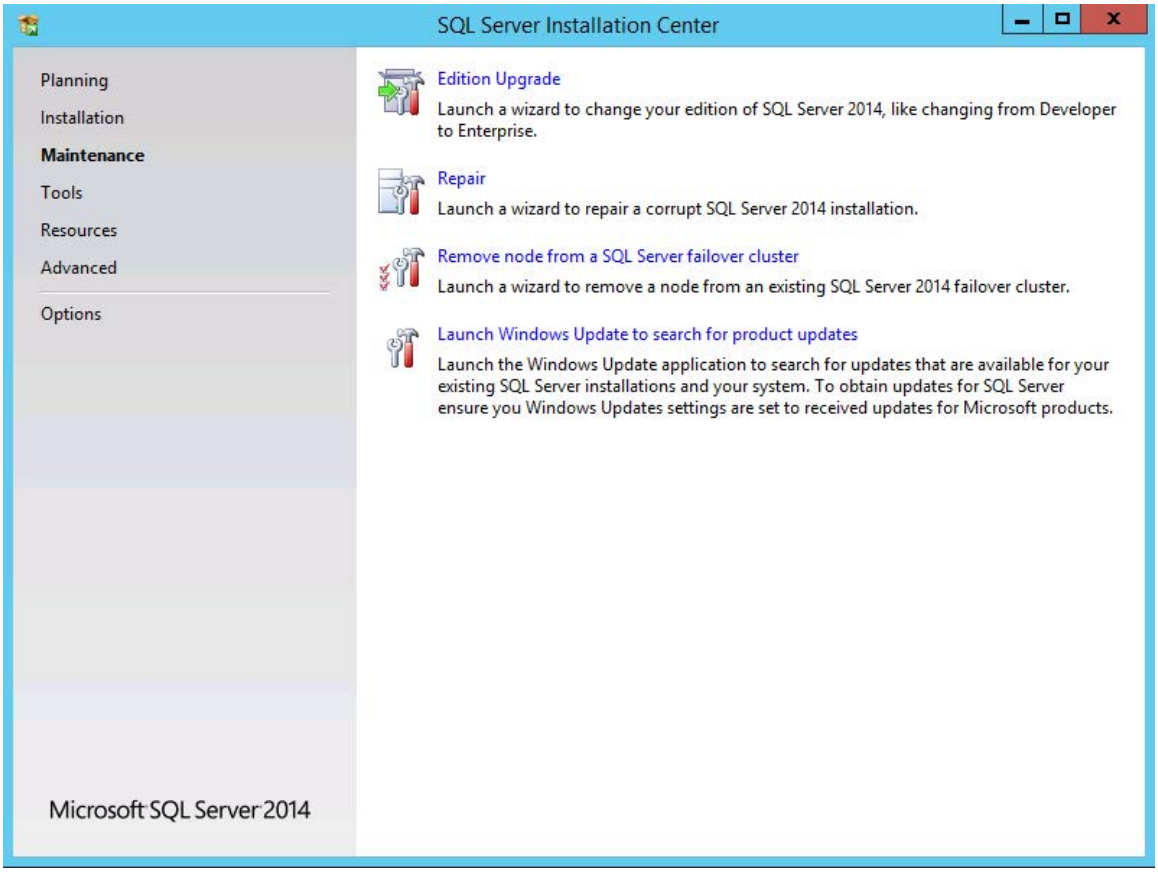
See the following Microsoft documentation on upgrading between editions called *Upgrade to a Different Edition of SQL Server 2014 (Setup)* at https://technet.microsoft.com/en-us/library/cc707783(v=sql.120).aspx

The EMS database is saved in the *C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf* file in the EMS host server. This file's size should remain below the 10 GB limit for Microsoft SQL Server Express.

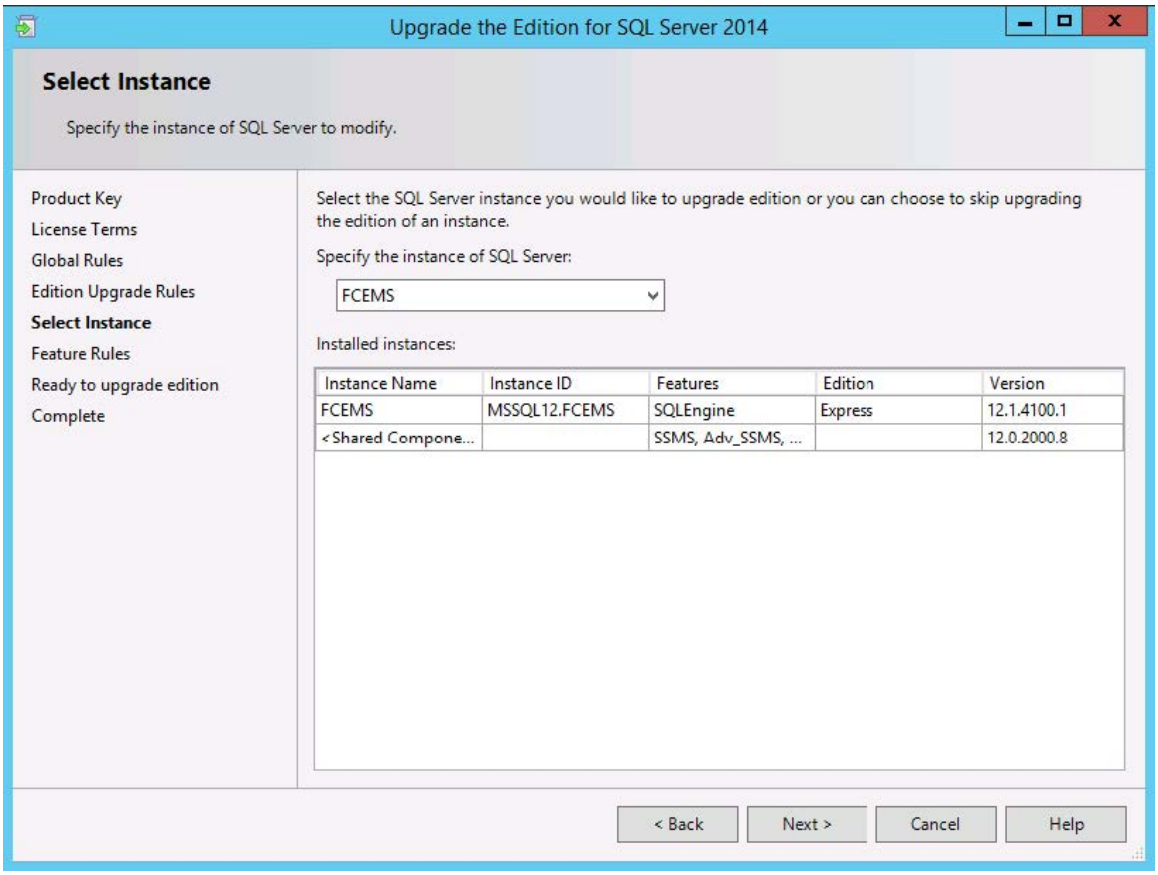
It is recommended to do a database edition upgrade outside normal production hours.

**To upgrade Microsoft SQL Server Express:**

1. Attach the SQL Server 2014 installation media to the FortiClient EMS for Chromebooks server.
   The installation media is a DVD or ISO file. If using the DVD, insert the DVD into the EMS host computer (host server). If your host server is a virtual machine, use the ISO file.
2. Run the SQL Server setup application wizard.
3. In the *SQL Server Installation Center* wizard, go to *Maintenance* > *Edition Upgrade*.




4. Enter the *product key*.
5. Accept the license terms, then click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.




7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

## Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS for Chromebooks after the upgrade to verify proper operations. A simple test may be to:

1. Connect FortiClient on one or two test endpoints to FortiClient EMS for Chromebooks.
2. Create a new custom group in FortiClient EMS for Chromebooks and add the test endpoints to it.
3. Create a new endpoint profile and assign it to the new custom group.
4. Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

# Uninstalling FortiClient EMS for Chromebooks

Use the *Programs and Features* pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS for Chromebooks.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

**To uninstall FortiClient EMS for Chromebooks:**

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

# Google Admin Console Setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

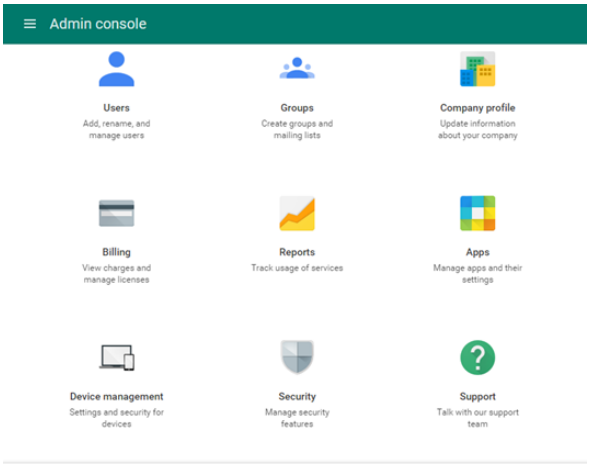
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 29.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 29.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 30.
4. Add the root certificate. See Adding root certificates on page 31.

## Logging into the Google Admin console

**To log into the Google Admin console:**

1. Log into the Google Admin console (https://admin.google.com) using your Google domain admin account. The Admin console displays.

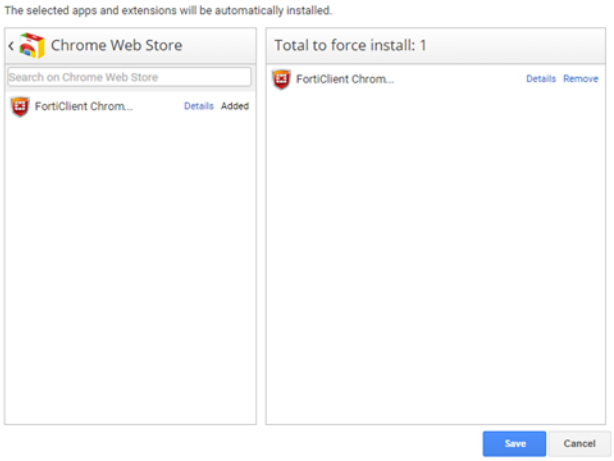



## Adding the FortiClient Web Filter extension

FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

**To add the FortiClient Web Filter extension:**

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name displays as *FortiClient Chromebook Web Filter Extension*.




# Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web access statistics sent from the FortiClient Web Filter extensions.

FortiClient EMS for Chromebooks is the profile server.

**To configure the FortiClient Web Filter extension:**

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *System Settings* > *EMS for Chromebooks*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443”}
}
```

3. In the Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.

   You can also view the current settings.
6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management* to view your configured Chrome apps.

# Adding root certificates

This section includes the following information:



## Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 68.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to the Google Admin console on page 33.

## Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, skip this section.

Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to the Google Admin console on page 33.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

## Enabling HTTP and HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTP-logging and HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS for Chromebooks.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```

## Adding SSL certificates to FortiAnalyzer

**To add SSL certificates to FortiAnalyzer:**

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

## Selecting certificates for HTTPS connections

**To select certificates for HTTPS connections:**

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate to use for HTTPS connections, and click *Apply*.

## Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

| Scenario | Certificate and CA | Where to Add Certificates |
|---|---|---|
| Allow the FortiClient Chromebook Web Filter extension to trust EMS | Public SSL certificate | • Add SSL certificate to FortiClient EMS for Chromebooks. |
| | SSL certificate not from a common CA | • Add SSL certificate to FortiClient EMS for Chromebooks.<br>• Add your certificate's root CA to the Google Admin console. |
| Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging | Public SSL certificate | • Add SSL certificate to FortiAnalyzer. |
| | SSL certificate not from a common CA | • Add SSL certificate to FortiAnalyzer.<br>• Add your certificate's root CA to the Google Admin console. |

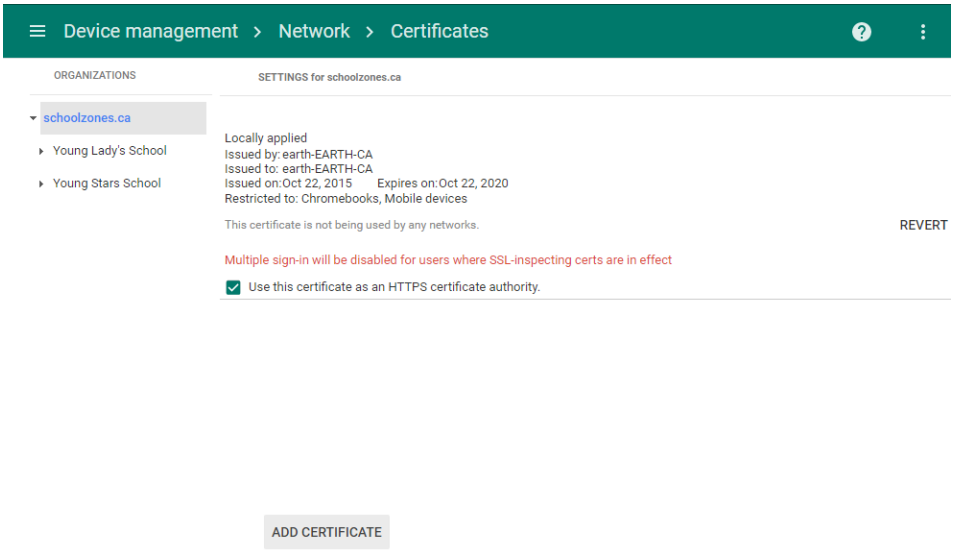
## Uploading root certificates to the Google Admin console

**To add root certificates:**

1. In the Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.

3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.




# Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

**To disable access to Chrome developer tools:**

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

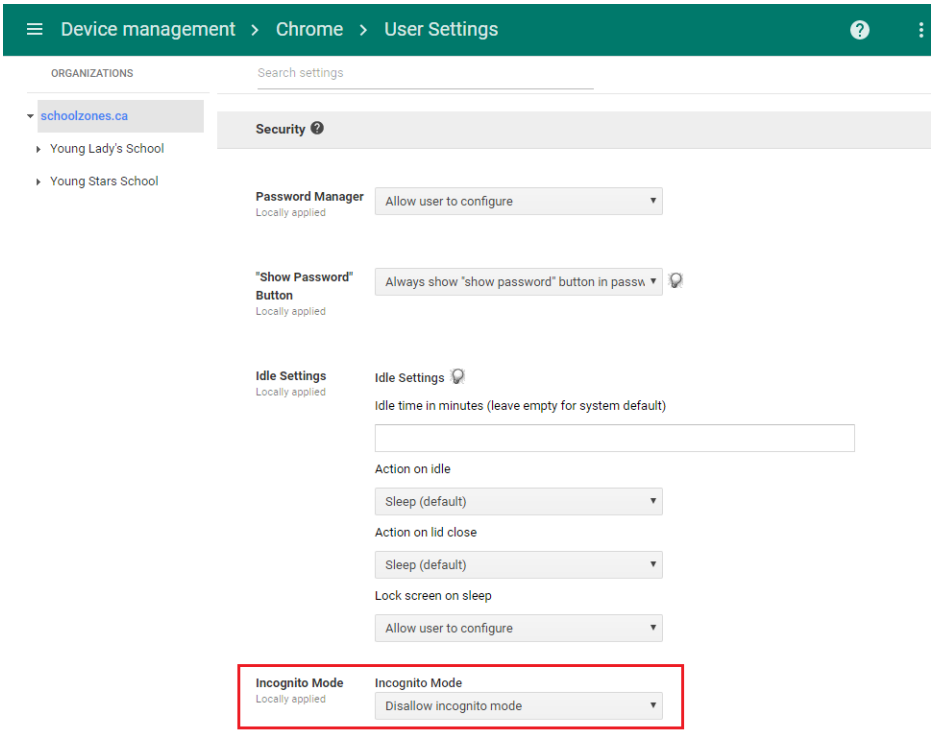
# Disallowing incognito mode

When users browse in incognito mode, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

**To disallow incognito mode:**

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.

3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.




4. Click *Save*.

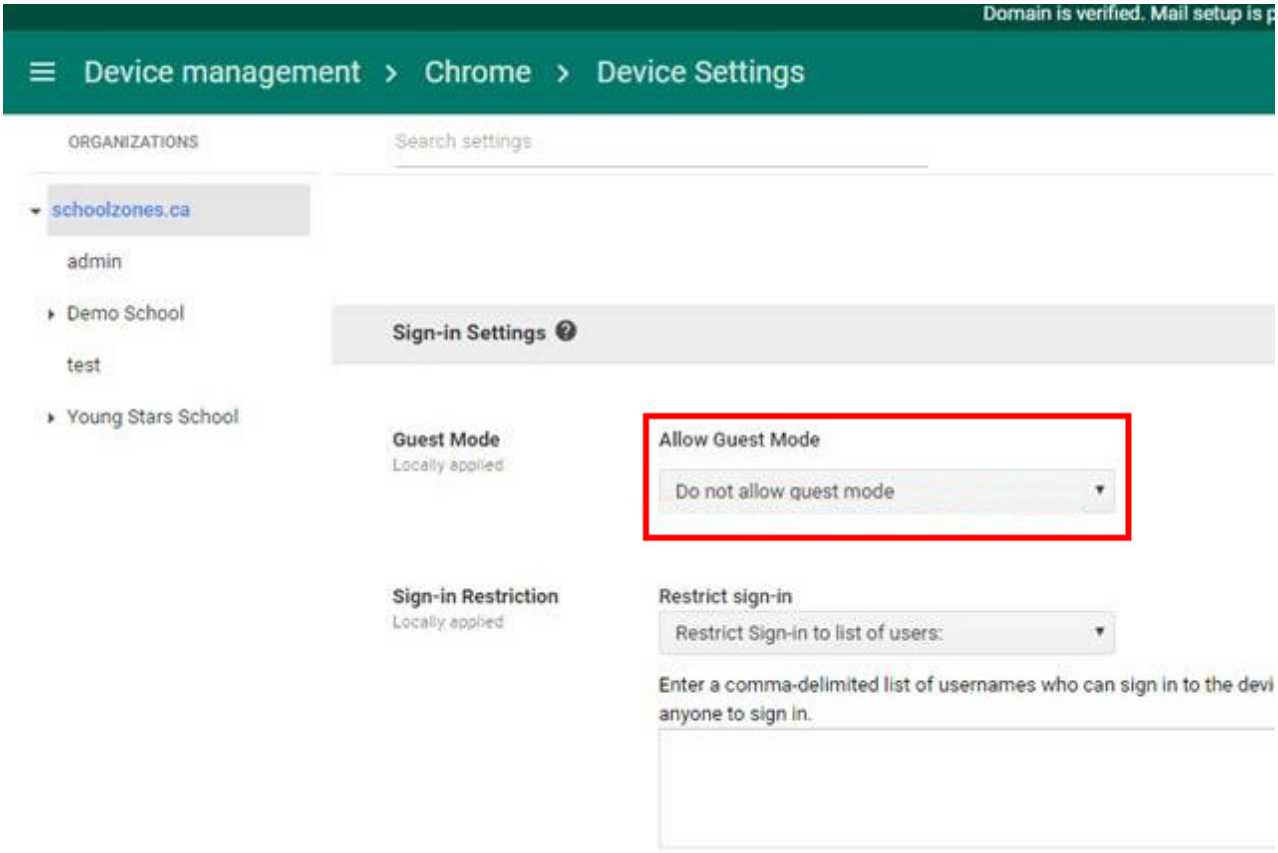
# Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

**To disallow guest mode:**

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.

3. Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.



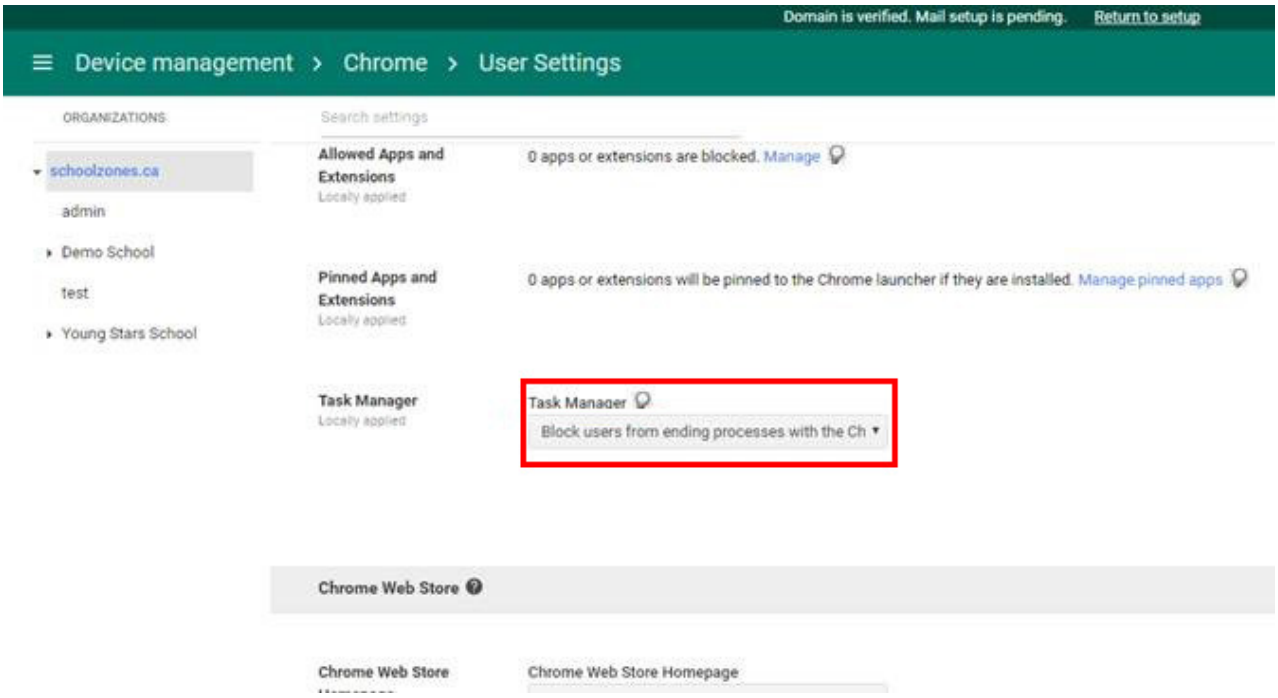

4. Click *Save*.

# Blocking Task Manager

Task Manager should be blocked for managed Google domains.

**To block Task Manager:**

1. In the Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.
2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown list.



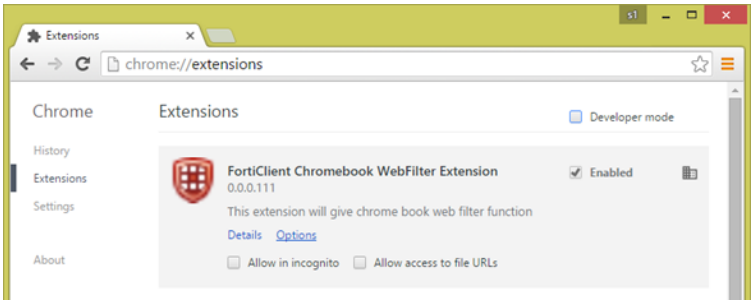

4. Click *Save*.

# Verifying the FortiClient Web Filter extension

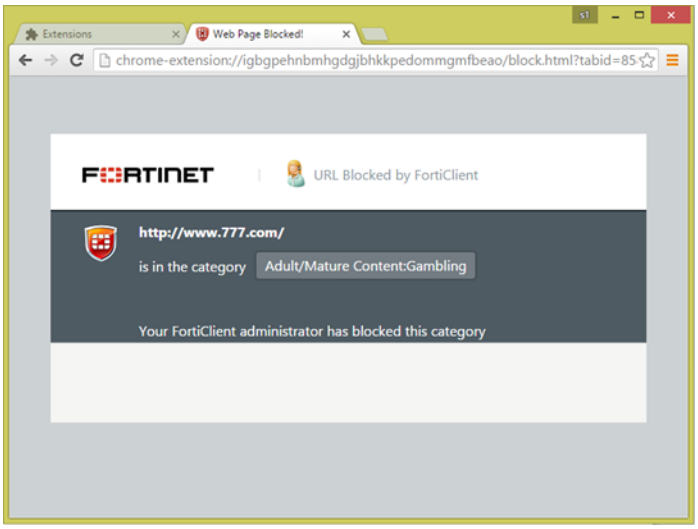
After you add the Google domain to FortiClient EMS for Chromebooks, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature has become available on the Chromebooks.

**To verify that the extension is installed:**

1. Open the Google Chrome browser.
2. Type the following in the address bar: *chrome://extensions*



3. Visit any gambling site, such as http://www.777.com, and confirm the site is blocked.



# Service Account Credentials

FortiClient EMS for Chromebooks requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS for Chromebooks or generate and use unique service account credentials, which is more secure.

The service account credentials must be the same in FortiClient EMS for Chromebooks and the Google Admin console.

This section describes how to configure default and unique service account credentials. See the following sections:


- Configuring default service account credentials on page 39
- Configuring unique service account credentials on page 40


## Configuring default service account credentials

FortiClient EMS for Chromebooks includes the following default service account credentials generated by the Google Developer console:

| Option | Default Setting | Where Used |
|---|---|---|
| Client ID | 102515977741391213738 | Google Admin console |
| Email address | account-1@forticlientwebfilter.iam.gserviceaccount.com | FortiClient EMS for Chromebooks |
| Service account certificate | A certificate in `.pem` format for the service account credentials | FortiClient EMS for Chromebooks |

The service account credentials are a set. If you change one credential, you must change the other two credentials.

### Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See Adding service account credentials to the Google Admin console on page 43.

# Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS for Chromebooks:

1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 40.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 43.
3. Add the unique service account credentials to FortiClient EMS for Chromebooks. See Adding service account credentials to EMS on page 44.

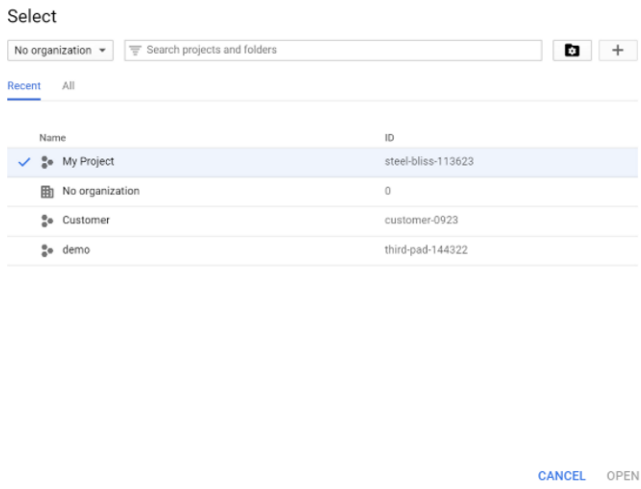
## Creating unique service account credentials

Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

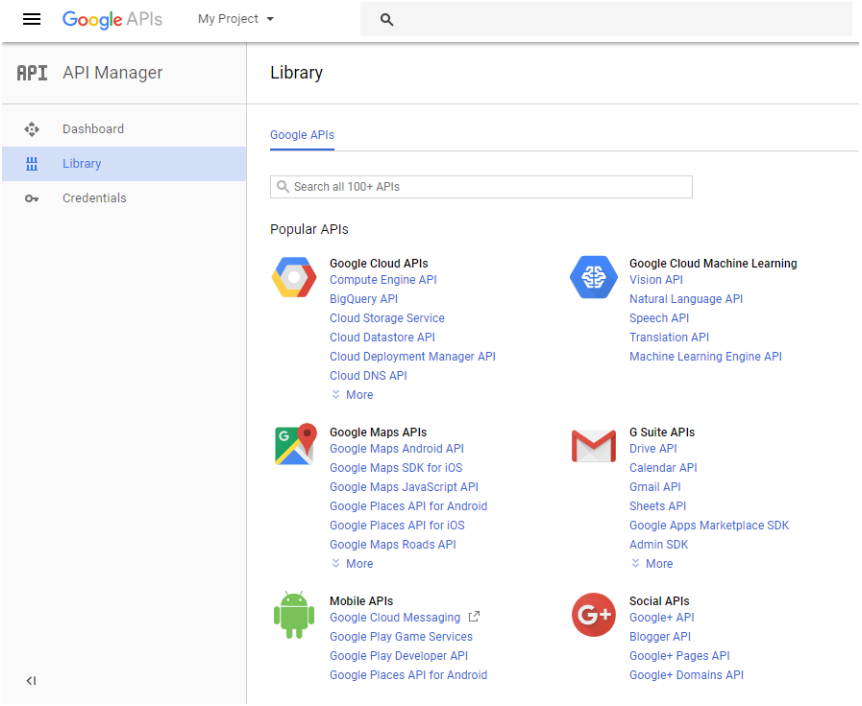
**To create a unique service account:**

1. Go to https://console.developers.google.com.
2. Log in with your G Suite account credentials.
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.

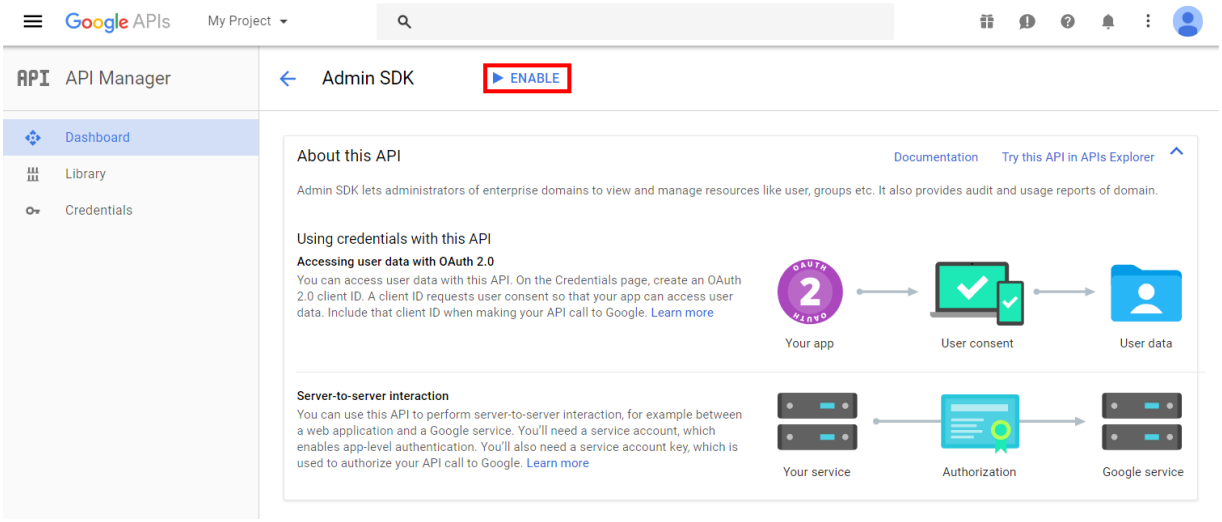



   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.

4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then go to the *Library* tab.
   b. Under *G Suite APIs*, click *Admin SDK*.

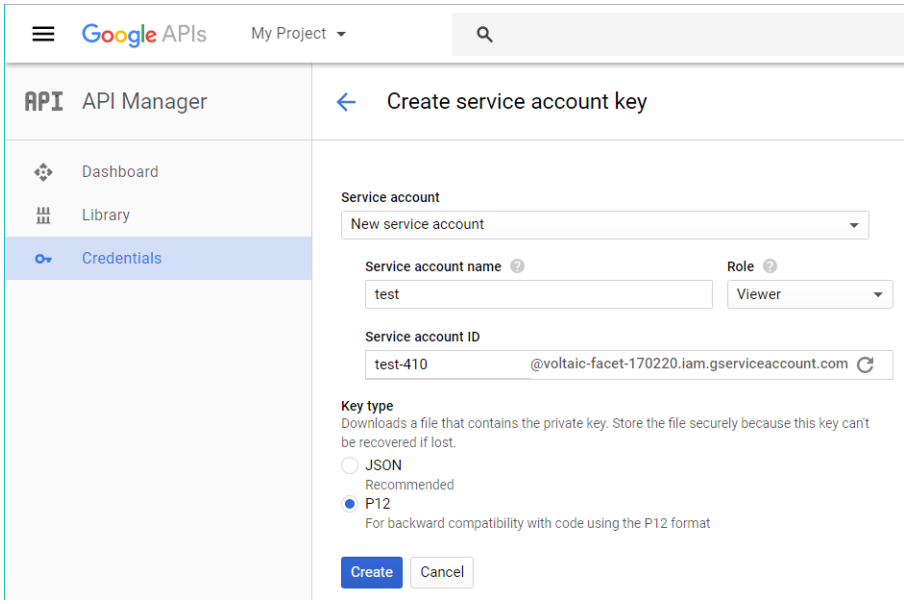



   c. Click *ENABLE*.



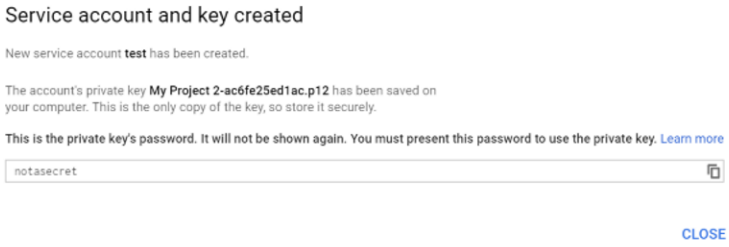

5. Create a service account:
   a. Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.
   b. From the *Service account* list, select *New Service Account*. Enter a service account name.
   c. From the *Role* list, select *Project* > *Viewer*.

**d.** Select *P12* as the *Key type* and click *Create*.

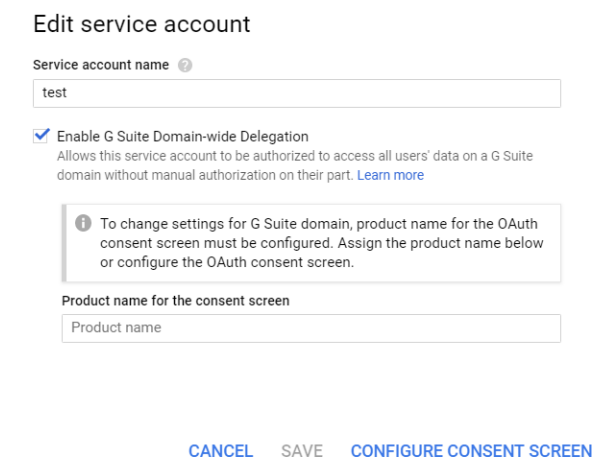



After you create the service account, a private key with the `P12` extension is saved on your computer.

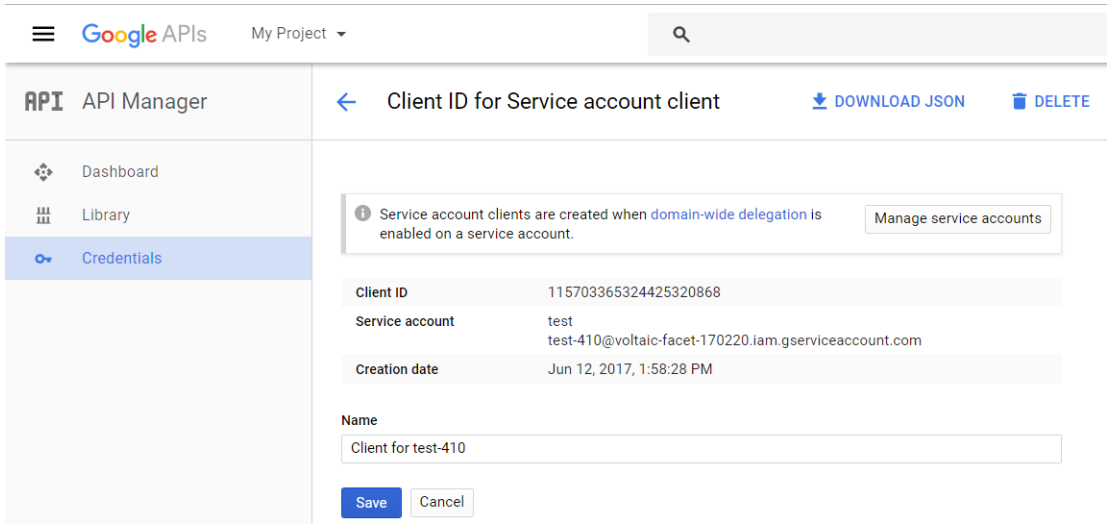
The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.




6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and select the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.




8. Click *Save*.
9. Click *View Client ID* to see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).




To use the private key in EMS, it needs to be converted to .pem format. You can use the following openssl command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
     serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

## Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

**To add the client ID:**

1. In the Google Admin console, go to *Security* > *Advanced settings* > *(you may need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the service account credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

   The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.
3. Click *Authorize*.

## Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS for Chromebooks.

**To add service account credentials:**

1. In FortiClient EMS for Chromebooks, go to *System Settings* > *EMS for Chromebook*.

   The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.
2. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

| | |
|---|---|
| ID | Type a new email address for the service account credentials. |
| Private key | Click *Browse* and select the certificate provided with the service account credentials. |

3. Click *Save*.
4. Update the client ID in the Google Admin console.

The service account credentials are a set. If you change one credential, you must change the other two credentials.

# GUI

The FortiClient EMS for Chromebooks GUI consists of the following areas:

- Banner
- Left pane
- Content pane

## Banner

| Option | Description |
|---|---|
| Bell icon | Click the bell icon to display all alert logs. |
| <Logged in username> | Click the dropdown list beside the <logged in username> to log out of FortiClient EMS for Chromebooks. |

## Left pane

The left navigation pane is used to display content in the right content pane.

| Option | | Description |
|---|---|---|
| Dashboard | | |
| | FortiClient Status | Displays a dashboard of information about all managed Chromebooks. |
| Google Domains | | |
| | All Users | Add and manage all users. |
| | Manage Domains | Manage domains. |
| | Domains | Add and manage users from domains. |
| Endpoint Profiles | | |
| | Manage Profiles | Create and assign profiles and manage profile updates for all profiles. |
| | Local Profiles | Create and assign profiles and manage profile updates for local profiles. |

| Option | | Description |
|---|---|---|
| Administration | | |
| | Administrators | Add and manage administrators. |
| | User Settings | Configure the inactivity timeout. |
| | Back up Database | Back up the FortiClient EMS for Chromebooks database. |
| | Restore Database | Restore the FortiClient EMS for Chromebooks database. |
| | Upgrade License | Upgrade or renew the FortiClient EMS license. |
| | Logs | View log messages generated by FortiClient EMS for Chromebooks and download raw logs. |
| System Settings | | |
| | Server | Change the IP address and port and configure other server settings for FortiClient EMS for Chromebooks. |
| | Logs | Specify what level of log messages to capture in FortiClient EMS for Chromebooks logs and when to automatically delete logs and alerts. |
| | Login Banner | Enable the pre-login banner to display a message to a user logging into FortiClient EMS for Chromebooks. |
| | EMS for Chromebooks | Configure settings specific to FortiClient EMS for Chromebooks, including adding service account credentials. |
| | EMS Alerts | Enable alerts for FortiClient EMS for Chromebooks events. |
| | SMTP Server | Set up an SMTP server to enable email alerts. |
| Help | | |
| | Getting Started | Provides access to links to the FortiClient EMS for Chromebooks *Release Notes, QuickStart Guide*, and other resources. |
| | Technical Documentation | Link to the FortiClient EMS for Chromebooks documentation. |
| | How-To Videos | Link to the Fortinet Video Library website. |
| | Forums | Link to Fortinet Customer Service and Support forum. |
| | Set up FortiClient EMS for Chromebooks | Link to a video showing the basic setup and functionality for FortiClient EMS for Chromebooks. |
| | Introduction to FortiClient EMS for Chromebooks | Link to an introductory video for FortiClient EMS for Chromebooks, which gives an overview of features, modes, and system requirements for FortiClient EMS for Chromebooks 1.0. |
| | How to License FortiClient EMS for Chromebooks | Link to a video showing how to license or renew FortiClient EMS for Chromebooks 1.0 with more endpoints. |

| Option | Description |
| --- | --- |
| Create Support Package | Create a support package to provide to the Fortinet technical support team for troubleshooting. |

# Content pane

The right content pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

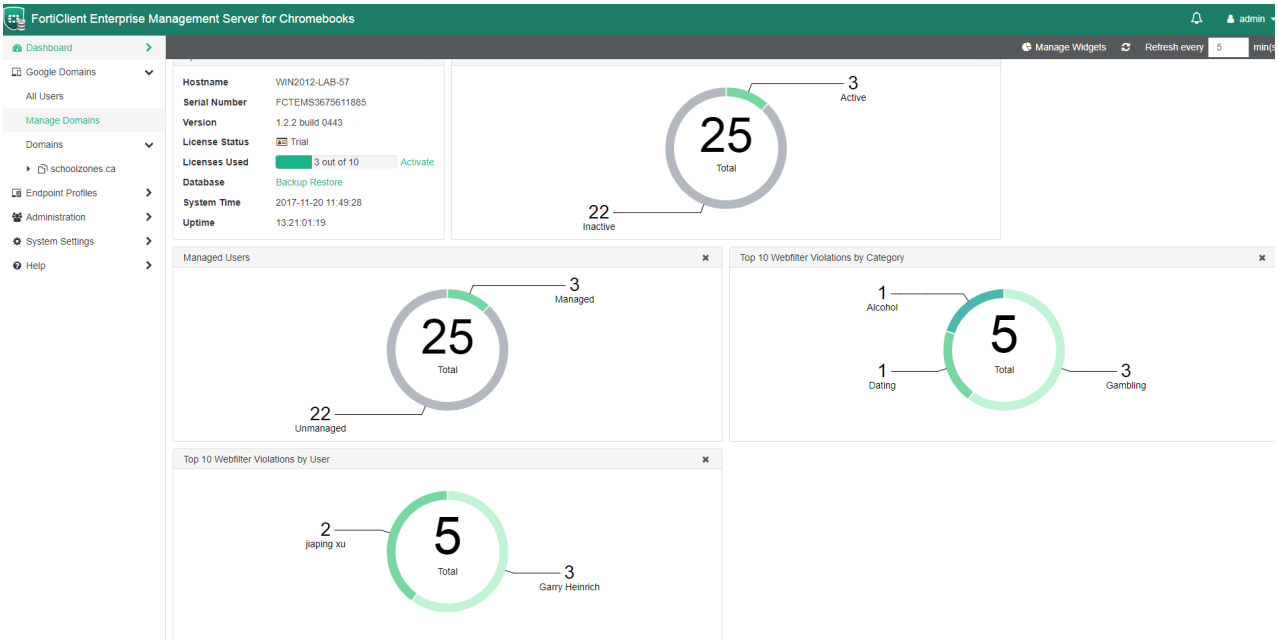
# Dashboard

You can use the Dashboard to view summary information about the system and endpoints.

## Viewing the FortiClient Status

**To view the FortiClient Status:**

1. In the left pane, click *Dashboard* > *FortiClient Status*.
   A *System Information* widget and charts and widgets of summary information display. See System Information widget on page 48 and FortiClient Status charts and widgets on page 49.




2. Click an event summary.
   The list of endpoints for the summary displays.
3. Click the *Back* button to return to the *FortiClient Status* pane.
4. Click a pie chart.
   The *Endpoints* content pane displays with more details about the endpoints related to the pie charts.

## System Information widget

The following information displays in the *System Information* widget:

| Option | Description |
|---|---|
| Hostname | Name of the computer on which FortiClient EMS for Chromebooks is installed. |
| Serial Number | Serial number for FortiClient EMS for Chromebooks. |
| Version | Version number for FortiClient EMS for Chromebooks. |
| License Status | Status of the license for FortiClient EMS for Chromebooks. Also displays a button for activating, upgrading, or renewing a license, depending on the license status.<br>If you have just installed EMS, click *Activate* to upload your license file. If you have a non-expired license, but want to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button is enabled for you to upload your new license file. See Licensing FortiClient EMS for Chromebooks on page 22. |
| Licenses Used | Number of licenses used out of the total number of available licenses. |
| Database | Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database. |
| System Time | Time and date used by the computer on which FortiClient EMS for Chromebooks is installed. |
| Uptime | Number of days, hours, minutes, and seconds FortiClient EMS for Chromebooks has been running. |

## FortiClient Status charts and widgets

FortiClient Status displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

| Option | Description |
|---|---|
| **User Charts** | |
| Active Users | This chart displays the active and inactive users. |
| Managed Users | This chart displays the managed and unmanaged users. |
| **Webfilter Charts** | |
| Top 10 Violations by Category | The chart displays the top ten web filter violations by category in the past few days. You can configure the number of days. Go to *System Settings* > *Logs*. |
| Top 10 Violations by User | The chart displays the top web filter violations by user in the past few days. You can configure the number of days. Go to *System Settings* > *Logs*. |
| **Others** | |
| System Information | This widget displays summary information for the system. |

# Google Domains

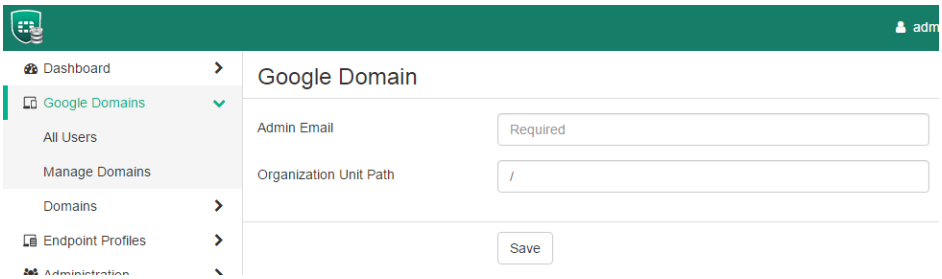
FortiClient EMS for Chromebooks needs to determine which devices to manage. Device information comes from the Google Admin console.



## Adding Google domains

**To add Google domains:**

1. Go to *Google Domains* > *Manage Domains*, and click the *Add* button. The *Google Domain* pane displays.




2. In the *Admin Email* box, type your Google domain admin email.
3. In the *Organization Unit Path* box, type the domain organization unit path.

/ stands for the root of the domain.

4. Click *Save*.
   The Google domain information and users are imported into FortiClient EMS for Chromebooks.

## Viewing domains

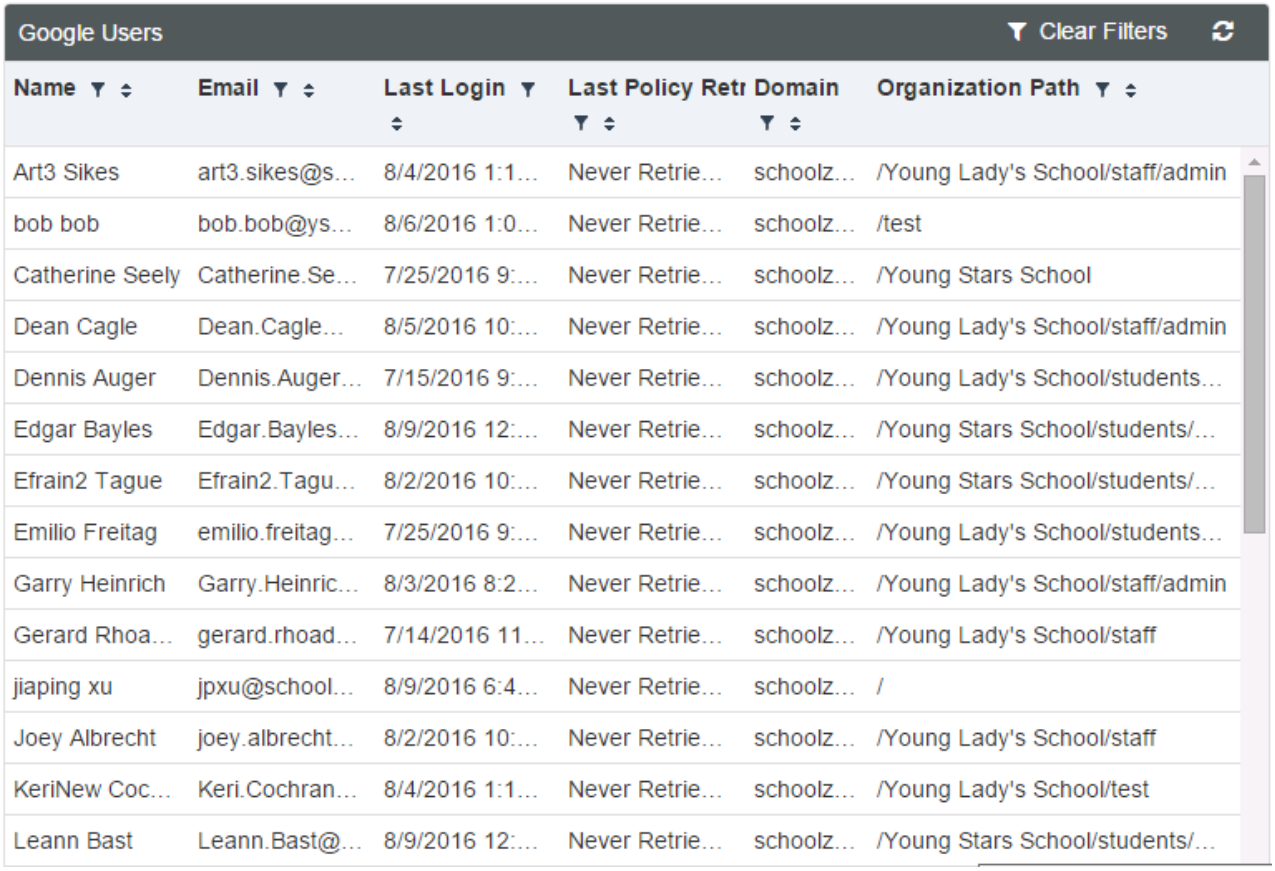
After you add domains to FortiClient EMS for Chromebooks, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

## Viewing the Google Users pane

You can view Google users' information in FortiClient EMS for Chromebooks.

**To view the Google Users pane:**

1. Go to *Google Domains* > *Domains* and click a domain. The list of Google users displays.




The following options are available in the toolbar:

| | |
|---|---|
| Clear Filter (filter icon) | Click the Clear Current Filter icon to clear the currently used filter. |
| Refresh | Click the Refresh icon to refresh the page. |

The following columns of information are displayed for Google users:

| | |
|---|---|
| Name | Chromebook user's name. |
| Email | Chromebook user's email address. |
| Last Login | Date and time when the user last logged into the domain. |
| Last Policy Retrieval | Date and time of the last endpoint profile retrieved by the Google Chromebook. |
| Domain | Name of the domain to which the user belongs. |

| | |
|---|---|
| Organizational Path | Organization path in the domain. |

## Viewing user details

You can view details about each user in a Google domain.

**To view user details:**

1. Go to *Google Domains* > *Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

### User Details

| Field | Information |
|---|---|
| Name | User's name. |
| Email | User's email address. |
| Last Login | Date and time when the user last logged into the domain. |
| Last Policy Retrieval | Date and time of the last endpoint profile retrieved by the Google Chromebook. |
| Organization Path | Organization path of the user in the domain. |
| Effective Policy | Name of the profile assigned to the user in the domain. |

### Client Statistics

| Charts | Information |
|---|---|
| Blocked Sites Distribution (past <number> days) | Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*. |
| Top 10 Site Categories by Distribution (Past <number> Days) | Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*. |

### Blocked Sites (Past <number> Days)

| Fields | Information |
|---|---|
| Time | Time the blocked site was visited. |

| Fields | Information |
|---|---|
| Threat | Threat type detected. |
| Client Version | Chromebook user's current version. |
| OS | Type of OS used by the Chromebook user. |
| URL | Blocked site's URL. |
| Port | Port number currently listening. |
| User Initiated | User initiated visitation to the blocked site. |

# Managing domains

You can manage domains from the *Google Domains* pane.

## Editing domains

**To edit domains:**

1. Go to *Google Domains* > *Domains* and select a domain.
2. Click the *Edit* button.
3. Edit the options and click *Save Changes*.

## Deleting domains

**To delete domains:**

1. Go to *Google Domains* > *Domains*, and select a domain.
2. Click the *Delete* button. A confirmation dialog displays.
3. Click *Yes*.

# Endpoint Profiles

You can use the default endpoint profile or create endpoint profiles for many configurations and situations.



## Configuring profiles

Profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

### Editing the default profile

You can edit the default profile to add or remove settings. You can revert to default settings by clicking *Revert to Default*.

**To edit the default profile:**

1. Go to *Endpoint Profiles* > *Local Profiles*, and click the *Default* profile.
2. Configure the settings on the tabs. See Profile references on page 57.
3. Click *Save* to save the profile.

### Adding new profiles

When you install FortiClient EMS for Chromebooks, a default profile is created. This profile is applied to any domains you add to FortiClient EMS for Chromebooks.

It is recommended to add Yandex search engine to the black list in the profile.

**To create new profiles:**

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.

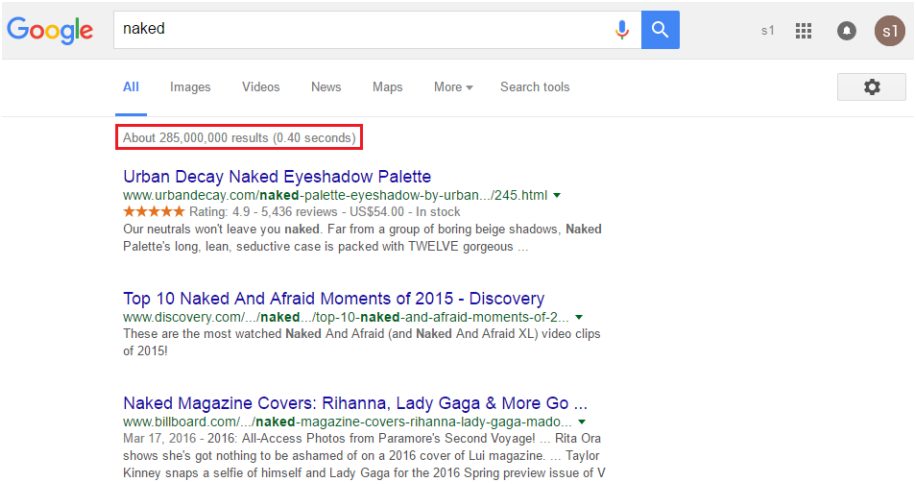
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

## Enabling/disabling Safe Search

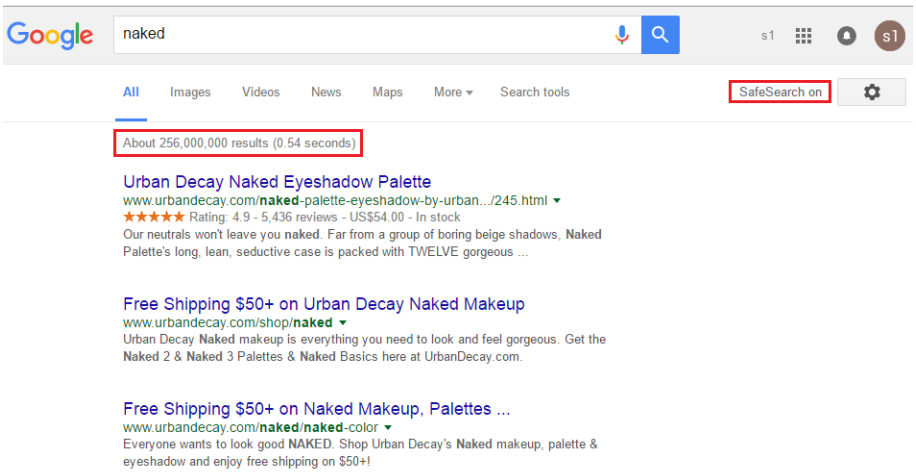
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS for Chromebooks supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS for Chromebooks controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:




Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.




**To enable or disable Safe Search:**

1. In FortiClient EMS for Chromebooks, in the *Endpoint Profiles* area, click the *Default* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

# Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view endpoint profiles and their settings.

**To view profiles:**

1. Go to *Endpoint Profiles* > *Manage Profiles*. The content pane displays the list of profiles.
2. Click a profile name, then click *Edit*. The settings display in the content pane.

# Assigning profiles to Google Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

**To assign profiles:**

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

# Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

## Editing profiles

When you edit a profile assigned to domains, the changes are automatically pushed to the Chromebooks when you save the profile.

**To edit profiles:**

1. Go to *Endpoint Profiles*, and select a profile.
2. Click *Edit*. The profile settings display in the content pane.
3. Edit the settings. See Profile references on page 57.
4. Click *Save*. If the profile is assigned to domains, the changes are pushed to the domains.

## Cloning profiles

**To clone profiles:**

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile displays in the content pane.
3. In the *Profile Name* box, type a name for the profile.
4. Configure the settings on the tabs. See Profile references on page 57.
5. Click *Save*.

## Deleting profiles

You cannot delete the default profile.

**To delete profiles:**

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Click desired profile, then click the *Delete* button. A popup displays.
3. Click *Yes*. The profile is deleted.

# Profile references

This section contains descriptions of the tabs and options used to configure profiles.

## Web Filter

| Configuration | | Description |
|---|---|---|
| Web Filter | | Enable or disable web filtering. |
| General | | |
| | Log All URLs | Enable to log all URLs. |
| | Log User Initiated Traffic | Enable to log user initiated traffic. |
| | Enable Safe Search | Enable safe search.<br>When safe search is enabled, the endpoint's Google search is set to *Restricted mode*, and YouTube access is set to *Strict Restricted access*. To set YouTube access to *Moderate Restricted* or *Unrestricted YouTube access*, you can disable Safe search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS for Chromebooks. |

| Configuration | | Description |
|---|---|---|
| Site Categories | | Select to enable site categories. When site categories are disabled, FortiClient is protected by the exclusion list.<br>See the FortiGuard website for descriptions of the available categories and subcategories. |
| | Adult/Mature Content | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | Bandwidth Consuming | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | General Interest-Business | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | General Interest-Personal | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | Potentially Liable | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | Security Risk | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |

| Configuration | | Description |
|---|---|---|
| | Unrated | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor |
| | Rate IP Addresses | Enable to rate all IP addresses. |
| **Exclusion List** | | |
| Action | | Select one of the following actions:<br>• Allow<br>• Block<br>• Monitor |
| URL | | Enter specific URLs to allow, block, or monitor. |
| Type | | Select one of the following types:<br>• Simple<br>• Wildcard<br>• Regular Expression<br>Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used. |

## System Settings

| Configuration | Description |
|---|---|
| **Log** | Specify FortiClient log settings. |
| Level | Select one of the following:<br>• Disabled<br>• Emergency: The system becomes unstable.<br>• Alert: Immediate action is required.<br>• Critical: Functionality is affected.<br>• Error: An error condition exists and functionality could be affected.<br>• Warning: Functionality could be affected.<br>• Notice: Information about normal events.<br>• Info: General information about system operations.<br>• Debug: Debug FortiClient. |
| Upload Logs to FortiAnalyzer/FortiManager | Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname. |

| Configuration | | Description |
|---|---|---|
| | IP Address/Hostname | Enter the IP address. When connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Otherwise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*. |
| | Upload Schedule (minutes) | Configure the upload schedule in minutes. |
| | Log Retention (days) | Configure the duration of time to retain logs in days. |
| | Compress Logs | Enable to compress logs. |

# Administration

## Administrators

This section describes the default user accounts and permissions for FortiClient EMS for Chromebooks. It also describes how to change the administrator password and configure Windows users.

### Default user account and permissions

The default user named *admin* has complete access to all FortiClient EMS for Chromebooks permissions, including modification, user permissions, approval, discovery, and deployment.

### Viewing users

You can view the default *admin* user and all users added to FortiClient EMS for Chromebooks.

**To view users:**

1. Go to *Administration* > *Administrators*.
   The following information displays:

| | |
|---|---|
| Add | Add a new user. |
| Refresh | Refresh the list of users. |
| Name | The username. |
| Type | Type of user. |
| Permissions | Type of user access. |

### Configuring Administrators

The following configuration options are available under *Administrators*:

- Changing the admin password on page 61
- Configuring Windows user accounts on page 62

#### Changing the admin password

By default, the *admin* user account has no password. You should add a password to increase security.

**To change the admin password:**

1. Go to *Administration* > *Administrators*.
2. Select the *admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.

### Configuring Windows user accounts

You can configure Windows users to have no access or administrator access to FortiClient EMS for Chromebooks.

The Windows users list is derived from the server on which FortiClient EMS for Chromebooks is installed. If you want to add more Windows users, you must add them to the server.

**To configure Windows users:**

1. Go to *Administration* > *Administrators*.
2. Click the *Add* button from the toolbar.
3. Perform one of the following actions:
   a. Select the specific domain access for the user. See Default user account and permissions on page 61.
   b. Configure the permissions.
4. Click *Save*.

## Administrators reference

This section contains descriptions of the fields used to configure *Administrators*.

### Windows users

Following is a description of the fields in *Administration* > *Administrators* > *Add*.

| Option | Description |
|---|---|
| User | Select the Windows user to configure permissions for FortiClient EMS for Chromebooks. |
| Super Administrator permissions | Enable the super administrator feature to give the new Windows user super administrator permissions. |
| Comment | Enter optional comments/information for the Windows user. |
| Domain Access | Select or add access to a domain for the Windows user and configure their permissions.<br>If you choose one or more domains in the domain access field, you must select specific permissions. |

| Option | Description |
|---|---|
| General Permissions | Use the settings to configure permissions to FortiClient EMS for Chromebooks for the selected Windows user. |
| Create/Delete filters | Select to allow the Windows user to create and delete filters. Clear to disable this permission. |
| Policy Permissions | |
| Assign/Unassign policies | Select to allow the Windows user to assign to endpoints and unassign profiles from domains and manage custom groups. Clear to disable this permission. |
| Create/Update/Delete policies | Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission. |

# Configuring User Settings

**To configure User Settings:**

1. Go to *Administration* > *User Settings*.
2. Set the following option:

| | |
|---|---|
| Inactivity timeout | Specify how long to keep inactive users logged into FortiClient EMS for Chromebooks. When the time expires, the user is automatically logged out of FortiClient EMS for Chromebooks. Type 0 to keep inactive users logged into FortiClient EMS for Chromebooks indefinitely. |

3. Click *Save*.

# Database management

You can back up and restore the FortiClient EMS for Chromebooks database.

## Backing up the database

**To back up the database:**

1. Go to *Administration* > *Back up Database*.
2. Set the following options:

| | |
|---|---|
| Password | Type a password for backing up and restoring the database. |
| Confirm password | Retype the password to confirm it. |

3. Click *Back up*.
   The database is backed up.

## Restoring the database

**To restore the database:**

1. Go to *Administration* > *Restore Database*.
2. Click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, type the password used to back up the database.
5. Click *Restore*.

   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
6. Wait for the restored database to be reloaded.

# License upgrades or renewals

Contact Fortinet Support to upgrade or renew your FortiClient EMS for Chromebooks license. After you have the license file, you can add it to FortiClient EMS for Chromebooks.

**To upgrade or renew the FortiClient EMS for Chromebooks license:**

1. Go to *Administration* > *Upgrade License*. The *Upgrade License* pane displays.
2. Click *Activate*, then click *Browse* and locate the license key file.
3. Click *Upload*.

# Logs

You can view the log messages generated by FortiClient EMS for Chromebooks and download raw logs.

## Viewing logs

**To view log messages:**

1. Go to *Administration* > *View and Download Logs*.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

## Downloading logs

You can download the logs generated by FortiClient EMS for Chromebooks.

**To download logs:**

1. Go to *Administration* > *View and Download Logs*.
2. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

# System Settings

This section describes FortiClient EMS for Chromebooks settings.

## Configuring Server settings

FortiClient EMS for Chromebooks installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiClient EMS for Chromebooks.

**To configure Server settings:**

1. Go to *System Settings* > *Server*.
2. Configure the following options:

| | | |
|---|---|---|
| Listen on IP | | Displays the IP addresses for the FortiClient EMS for Chromebooks server. FortiClient connects to FortiClient EMS for Chromebooks on the specified IP address. |
| Use FQDN | | Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS for Chromebooks server. |
| | FQDN | Displayed when *Use FQDN* is turned on. Type the FQDN for the FortiClient EMS for Chromebooks server. FortiClient can connect using the specified IP address in the *Listen on IP Addresses* option or the specified FQDN. |
| Remote HTTPS access | | Specify settings for remote administration access to FortiClient EMS for Chromebooks.<br>Turn remote HTTPS access to FortiClient EMS for Chromebooks console on and off. When enabled, type a host name in the *Custom Host Name* box to let administrators use a browser and HTTPS to log into the FortiClient EMS for Chromebooks console. When disabled, administrators can only log into FortiClient EMS for Chromebooks console on the server. |
| | Pre-defined hostname | Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name. The name cannot be changed. |
| | Custom hostname | Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS for Chromebooks is installed. You can customize the host name. When you change the host name, the web server restarts. |
| | Redirect HTTP request to HTTPS | Available when *Remote Administration HTTPS Access* is turned on. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*. |

| | |
|---|---|
| SSL certificate | Displays the SSL certificate currently imported. If you have not imported an SSL certificate, a *No SSL certificate imported* message displays. |
| New SSL Certificate File | Upload a new SSL certificate. |
| New SSL Private Key | Upload a new SSL private key. |

3. Click *Save*.

# Configuring Logs settings

You can specify what level of log messages to capture in the logs for FortiClient EMS for Chromebooks. You can also specify when to automatically delete logs and alerts.

**To configure Logs settings:**

1. Go to *System Settings* > *Logs*.
2. Configure the following options:

| | |
|---|---|
| Log level | Select the level of messages to include in FortiClient EMS for Chromebooks logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS for Chromebooks logs. |
| Clear logs every | Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted. |
| Clear alerts every | Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted. |
| Clear web filter logs every | Type the number of days that you want to keep web filter logs. For example, if you type 30, web filter logs will be kept for 30 days. Any web filter logs older than 30 days are automatically deleted. |
| Clear now | Click to immediately delete all FortiClient EMS for Chromebooks logs or alerts. |

3. Click *Save*.

# Configuring the login banner

When you enable the login banner, a message appears prior to a user logging into EMS.

**To enable and configure a login banner:**

1. Go to *System Settings* > *Login Banner*.
2. Click *Enable login banner*.

3. In the *Message* box, type your message. The *Preview* section displays a preview of the message.
4. Click *Save*.

# Configuring EMS for Chromebooks

**To configure Settings:**

1. Go to *System Settings* > *EMS for Chromebooks*.
2. Configure the following options:

| | |
|---|---|
| Listen on port | Displays the default port for the FortiClient EMS for Chromebooks server. You can change the port by typing a new port number. FortiClient connects to FortiClient EMS for Chromebooks using the specified port number. |
| User inactivity timeout | Enter the number of hours after of inactivity after which to timeout the user. |
| Profile update interval | Specify the profile update interval (in seconds). |
| SSL certificate | Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, a *Replace* button displays. |
| Certificate | Browse and upload a new SSL certificate file. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 68. |
| Password | Configure a new SSL password. |
| Service account | Displays the service account ID currently in use. |
| Update service account | Update the service account with new credentials. |
| Reset service account | In the event your service account is broken, you can revert back to the default service account by clicking the *Reset* button. This restores the default service account. You need to *Save* the settings for the change to take effect. |
| ID | Available if the *Update service account* button is clicked. Enter a new service account ID. |
| Private key | Available if the *Update service account* button is clicked. Upload a new service account private key. |

3. Click *Save*.

## Adding SSL certificates to FortiClient EMS for Chromebooks

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with the Google Admin console.

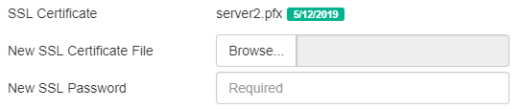
If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and the root certificate to the Google Admin console. See Adding root certificates on page 31.

**To add or replace SSL certificates:**

1. In FortiClient EMS for Chromebooks, go to *System Settings* > *EMS for Chromebooks*.
2. Beside *SSL certificate*, click *Update SSL certificate*.
3. Click *Browse* and locate the certificate file (<name>.pfx).
4. In the *Password* box, type the password.
5. Click *Test*.
6. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label is yellow; if it has expired, the label is red. Otherwise, it is green.




# Configuring EMS Alerts

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

**To configure email alerts and an SMTP server:**

1. Go to *System Settings* > *EMS Alerts*.
2. Set the following options to send an email when the following events happen:

| | | |
|---|---|---|
| New EMS version is available for deployment | | New EMS version is available. |
| | Remind me everyday for 2 weeks | Enable to remind you when new EMS versions are available everyday for two weeks. |
| EMS license is expired or about to expire | | Expiring or expired EMS license. |

3. Click *Save*.

   If you have not already set up an SMTP server, the GUI automatically prompts you to configure SMTP server settings. See Configuring SMTP Server settings on page 69.

# Configuring SMTP Server settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

**To configure SMTP Server settings:**

1. Go to *System Settings* > *SMTP Server*.
2. Set the following options:

| | |
|---|---|
| Server | Enter the SMTP server. |
| Port | Enter the port number. |
| Security | Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes become available. |
| Username | Enter the username. |
| Password | Enter the password. |
| From | Enter the email address to send the alerts from. |
| Reply-To | Enter the email address to send the replies to. |
| Subject | The sent e-mail alert's subject. |
| Recipients | Enter email address(es) to send alerts to. Click the + button to add more email addresses. |
| Test Subject | Test email's subject. |
| Test Message | Test email's message. |
| Test Recipient | Email address to send the test email to. |
| Send Test Email | Click the button to test the configured email settings. |

3. Click *Save*.

# Creating a Support Package

You can create a support package to provide to the Fortinet technical support team for troubleshooting. Creating a support package backs up your database, but clears all sensitive username and password fields.

**To create a support package:**

1. Go to *Help* > *Create Support Package*. The *Create Support Package* dialog box displays.
2. In the *Password* box, type your administrative password.
3. In the *Confirm Password* box, type your password again.
4. Click *Create Support Package*.